古典2次形式に関する考察(代数的数論 : 最近の進展とその背景)

AUTHOR(S):

久保田, 富雄

CITATION:

久保田, 富雄. 古典2次形式に関する考察(代数的数論 : 最近の進展とその背景). 数理解析研究所講究録 1993, 844: 58-73

ISSUE DATE:

1993-06

URL:

http://hdl.handle.net/2433/83603

数理解析研究所講究録
844巻 1993年 58-73

古典2次形式に関する考察

名大理　久保田　富雄
(Tomio Kubota)

代数体の巡回拡大体 K/F においては，至るところ local norm である F の元は global norm である．これは norm theorem, principal genus theorem, あるいは巡回拡大体の Hasse 原理などと呼ばれる定理であって，代数的整数論に種々の形で登場する．

また，最近になって，この principal genus theorem の持つ意味を，さらに1つ付け加えることができた．それは，ベキ剰余の相互法則と，一般の Artin の相互法則との gap を同定理がちょうど表しているということである．ただし，その際，定理は相対2次体のものに限ってよい．言い換えれば，一般代数体の2元（あるいは3元斉次）2次形式の Hasse 原理だけで十分である．

そこで，あらためて，principal genus theorem がどの様な性格のものであるかを検討してみたところ，相当に根が深いらしい1つの疑問に行き当たった．それは，2元形式の場合ですら，一般代数体においては，local な解から global な解を実際に構成するという形の証明が全くないということである．たとえば，類体論の第1，第2不等式が証明されれば副産物として一般の principal genus theorem が得られるし，また，同定理を多元環の splitting に関する Hasse 原理としてとらえ，多元環のゼータ関数を用いて証明することもでき，それによって類体論の別の形の構成法があたえられる．しかし，これらの証明はすべて背理法的で，定理のなりたつ原因が目に見えないのである．

有理数体上の２次体に関する principal genus theorem は Gauss の２次形式論の基本定理の１つであった．また，Legendre も Gauss に先立って，同定理の別の方法による証明を発表している．これらの証明においては，有理数体の場合ではあるが，local な解から global な解をはっきり構成している．しかもその方法は大変面白く，また見通しがよく，十分な一般性を持っているように見える．ところが，それを代数体に拡張しようとすると，２次体上においてすらうまく行かないのである．

この事実は，代数的整数論の身近な基礎理論の中に，いまだに十分解明されていない大きな部分が残っていることを示すのではないかと考えられるので，ここで問題提起しておきたい．

ベキ剰余の相互法則と，一般のArtin の相互法則との関係における principal genus theorem の意味については，”数学 ”，44-1, (1992), に論説として書いておいたので，ここでは，古典的な２次形式論で用いられた principal genus theorem の証明の紹介を主眼とする．そのため，まず Gauss の２次形式論を ideal 論を知っている立場から理解する方法を述べ，次に，Gauss と Legendre の方法による principal genus theorem の証明を解説する．Gauss の２次形式論は難解と言われているが，２，３ の定義と公式の意味の種明しを行えば，簡単に理解できるものなのである．

なお，本稿の内容は，古田孝臣氏の研究と関連が深い．特に，２次形式の composition に関する記号は，同氏によって工夫されたものを多く用いた．（c.f. Y.Furuta, Gaussian composition of congruence classes, Sci. Rep. Kanazawa Univ., 37 - 1, (1992), 1 - 22.）

Ｓｅｃｔｉｏｎ １．　２次形式の composition.

Binary な２次形式の Gauss 式の composition を定義する．定義に際し

ては，文字が何を表すかを決めておく必要はない．

定義（Gauss の composition） 2次形式 $f_3(x, y) = Ax^2 + Bxy + Cy^2$ が2つの2次形式

$$f_1 = a_1x^2 + b_1xy + c_1y^2 \quad \text{および} \quad f_2 = a_2x^2 + b_2xy + c_2y^2$$

の行列 $P = \begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix}$, $Q = \begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix}$ による（あるいは4つずつの2組の文字 $p_1, p_2, p_2', p_3;\ q_1, q_2, q_2', q_3$ による）composition であるとは，

$$X = p_1x_1x_2 + p_2x_1y_2 + p_2'y_1x_2 + p_3y_1y_2 = (x_1, y_1)\begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

$$Y = q_1x_1x_2 + q_2x_1y_2 + q_2'y_1x_2 + q_3y_1y_2 = (x_1, y_1)\begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

とおくとき，

$$f_1(x_1, y_1)f_2(x_2, y_2) = f_3(X, Y).$$

のなりたつことをいう．特に $f_1 = f_2 = f$ のとき，f_3 を f の duplication という．

この composition は ideal の乗法を2次形式で表現したものになっている．それをここで示す．

判別式が D である2次体を F とし，α_1, α_2 を F の ideal **a** の1組の **Z** 上の基底とする．このことを $\mathbf{a} = [\alpha_1, \alpha_2]$ とあらわす．このように基底を1つ定められた ideal に2次形式

$$f(x, y) = ax^2 + bxy + cy^2 = (N\mathbf{a})^{-1}(\alpha_1x + \alpha_2y)(\alpha_1^{\sigma}x + \alpha_2^{\sigma}y)$$

を対応させる．2次体の nontrivial automorphism を σ であらわす．**a** は α_1 と α_2 の最大公約 ideal で，$\alpha_1x + \alpha_2y$ の内容 ideal であるから，f

の係数 a, b, c の最大公約数は 1 で，f は primitive form である．また f の判別式 $b^2 - 4ac$ は D である．一般に α_1, α_2 が **a** の生成元であるとき，それらを用いて作った f は primitive で，その判別式は α_1, α_2 が基底であるとき，またそのときに限り D に等しい．

$\mathbf{a} = [\alpha_1, \alpha_2]$, $\mathbf{b} = [\beta_1, \beta_2]$ を F の 2 つの ideal とし，対応する 2 次形式をそれぞれ

$$f_1 = a_1x^2 + b_1xy + c_1y^2 = (N\mathbf{a})^{-1}(\alpha_1x + \alpha_2y)(\alpha_1^{\sigma}x + \alpha_2^{\sigma}y),$$
$$f_2 = a_2x^2 + b_2xy + c_2y^2 = (N\mathbf{b})^{-1}(\beta_1x + \beta_2y)(\beta_1^{\sigma}x + \beta_2^{\sigma}y)$$

とする．**c** の 1 組の基底を γ_1, γ_2 とすれば，Z の元 p_1, p_2, p_2', p_3; q_1, q_2', q_2, q_3 が存在して

$$\alpha_1\beta_1 = p_1\gamma_1 + q_1\gamma_2, \qquad \alpha_1\beta_2 = p_2\gamma_1 + q_2\gamma_2,$$
$$\alpha_2\beta_1 = p_2'\gamma_1 + q_2'\gamma_2, \qquad \alpha_2\beta_2 = p_3\gamma_1 + q_3\gamma_2$$

がなりたつ．従って

$$(*) \qquad (\alpha_1x_1 + \alpha_2y_1)(\beta_1x_2 + \beta_2y_2)$$
$$= \alpha_1\beta_1x_1x_2 + \alpha_1\beta_2x_1y_2 + \alpha_2\beta_1y_1x_2 + \alpha_2\beta_2y_1y_2$$

の右辺は $\gamma_1X + \gamma_2Y$, ただし

$$X = p_1x_1x_2 + p_2x_1y_2 + p_2'y_1x_2 + p_3y_1y_2 = (x_1, y_1)\begin{pmatrix} p_1 & p_2 \\ p_2' & p_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

$$Y = q_1x_1x_2 + q_2x_1y_2 + q_2'y_1x_2 + q_3y_1y_2 = (x_1, y_1)\begin{pmatrix} q_1 & q_2 \\ q_2' & q_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

となる．$(N\mathbf{c})^{-1}(\gamma_1X + \gamma_2Y)(\gamma_1^{\sigma}X + \gamma_2^{\sigma}Y) = AX^2 + BXY + CY^2 = f_3(X, Y)$ とおけば，(*) の両辺の $1 + \sigma$ ベキをとって $(N\mathbf{c})^{-1} = (N\mathbf{a}_1\mathbf{a}_2)^{-1}$ をかけることにより，

$$f_1(x_1, y_1)f_2(x_2, y_2) = f_3(X, Y)$$

となって，f_1, f_2, f_3 は，それぞれ **a**, **b**, **c** = **ab** という ideal から作ったものになっている．**c** = **ab** により，行列

$$\begin{pmatrix} p_1 & p_2 & p_2' & p_3 \\ q_1 & q_2 & q_2' & q_3 \end{pmatrix}$$

の 2 次の小行列式は 1 以外に公約数を持たない．

2 次形式の composition を具体的に計算するため，Gauss は公式を作った． それを duplication の場合について，ここで説明する．

命題（Duplication の計算）2 次形式 $f = ax^2 + bxy + cy^2$ の係数が他の量 $p_1, p_2, p_3; q_1, q_2, q_3$ によって

$$a = \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}, \quad b = \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix}, \quad c = \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix}$$

と表されるならば，

$$A = -\begin{vmatrix} q_1 & q_2 \\ q_2 & q_3 \end{vmatrix}, \quad B = \begin{vmatrix} p_1 & q_2 \\ p_2 & q_3 \end{vmatrix} + \begin{vmatrix} q_1 & p_2 \\ q_2 & p_3 \end{vmatrix}, \quad C = -\begin{vmatrix} p_1 & p_2 \\ p_2 & p_3 \end{vmatrix}$$

とおくとき， $g(x, y) = Ax^2 + Bxy + Cy^2$ は $P = \begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix}$,

$Q = \begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix}$ による f の duplication である．すなわち，

$$X = p_1x_1x_2 + p_2x_1y_2 + p_2y_1x_2 + p_3y_1y_2 = (x_1, y_1)\begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

$$Y = q_1x_1x_2 + q_2x_1y_2 + q_2y_1x_2 + q_3y_1y_2 = (x_1, y_1)\begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

について， $g(X, Y) = f(x_1, y_1)f(x_2, y_2)$ がなりたつ．

このとき $b^2 - 4ac = B^2 - 4AC$ もなりたつ．

これはもちろん，代入して計算すれば証明できる．しかし，それでは意味がわからないので，内容が理解できる形で命題を導き出してみる．

そのために，

$$f = ax^2 + bxy + cy^2 = a(x - \alpha y)(x - \alpha^\sigma y)$$

をとったとき，

$$X = p_1x_1x_2 + p_2x_1y_2 + p_2y_1x_2 + p_3y_1y_2 = (x_1,\ y_1)\begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

$$Y = q_1x_1x_2 + q_2x_1y_2 + q_2y_1x_2 + q_3y_1y_2 = (x_1,\ y_1)\begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

について，

$$A(X - \gamma Y)(X - \gamma^\sigma Y) = AX^2 + BXY + CY^2 = g(X,\ Y)$$

$$= f(x_1,\ y_1)f(x_2,\ y_2) = a(x_1 - \alpha y_1)(x_1 - \alpha^\sigma y_1)\cdot a(x_2 - \alpha y_2)(x_2 - \alpha^\sigma y_2)$$

がなりたつように，種々の量を決めて行く．

$$c_1 = p_1 - \gamma q_1,\quad c_2 = p_2 - \gamma q_2,\quad c_3 = p_3 - \gamma q_3$$

とおけば，

$$X - \gamma Y = c_1x_1x_2 + c_2x_1y_2 + c_2y_1x_2 + c_3y_1y_2$$

$$= x_1(c_1x_2 + c_2y_2) + y_1(c_2x_2 + c_3y_2).$$

これがさらに1次因子に分解されるのだから，

$$\begin{vmatrix} c_1 & c_2 \\ c_2 & c_3 \end{vmatrix} = \begin{vmatrix} p_1 - \gamma q_1 & p_2 - \gamma q_2 \\ p_2 - \gamma q_2 & p_3 - \gamma q_3 \end{vmatrix} = 0$$

である．これより，まず $A\gamma^2 + B\gamma + C = 0$ となるから，ここで

$$A = -\begin{vmatrix} q_1 & q_2 \\ q_2 & q_3 \end{vmatrix},\quad B = \begin{vmatrix} p_1 & q_2 \\ p_2 & q_3 \end{vmatrix} + \begin{vmatrix} q_1 & p_2 \\ q_2 & p_3 \end{vmatrix},\quad C = -\begin{vmatrix} p_1 & p_2 \\ p_2 & p_3 \end{vmatrix}$$

と固定して先へ進む．

$$\frac{p_2 - \gamma q_2}{p_1 - \gamma q_1} = \frac{p_3 - \gamma q_3}{p_2 - \gamma q_2} = -\lambda$$

とおけば

$$X - \gamma Y = x_1(c_1x_2 - \lambda c_1y_2) + y_1(-\lambda c_1x_2 + \lambda^2 c_3y_2)$$

$$= c_1(x_1 - \lambda y_1)(x_2 - \lambda y_2).$$

従って，必要なら α と α^σ を交換して $\lambda = \alpha$. さらに

$$\begin{vmatrix} p_1 - \gamma q_1 & p_2 - \gamma q_2 & p_3 - \gamma q_3 \\ p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \end{vmatrix} = 0$$

より

$$\begin{vmatrix} 1 & -\alpha & \alpha^2 \\ p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \end{vmatrix} = 0$$

となり，

$$\begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}\alpha^2 + \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix}\alpha + \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix} = 0.$$

そこで

$$ha = \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}, \quad hb = \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix}, \quad hc = \begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix}$$

とおけば，$g(X, Y) = f(x_1, y_1)f(x_2, y_2)$ がなりたつように h を決めることができる．そのために $x_1^2x_2^2$ の係数の一致 $Ap_1^2 + Bp_1q_1 + Cq_1^2 = a^2$ がなりたつ条件を求めると，A, B, C を定めた式および

$$Ap_1^2 + Bp_1q_1 + Cq_1^2 = q_1^2(A(\frac{p_1}{q_1})^2 + B\frac{p_1}{q_1} + C)$$

より

$$Ap_1^2 + Bp_1q_1 + Cq_1^2 = -q_1^2\begin{vmatrix} p_1 - \frac{p_1}{q_1}q_1 & p_2 - \frac{p_1}{q_1}q_2 \\ p_2 - \frac{p_1}{q_1}q_2 & p_3 - \frac{p_1}{q_1}q_3 \end{vmatrix}$$

$$= -\begin{vmatrix} 0 & p_2q_1 - p_1q_2 \\ p_2q_1 - p_1q_2 & p_3q_1 - p_1q_3 \end{vmatrix} = (p_1q_2 - p_2q_1)^2 = \begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix}^2 = g^2a^2.$$

であるから，

$$h^2a^2 = a^2$$

が得られる．これは $h = 1$ で，従って a, b, c が命題にいうとうりの値に

なったときには確かに満たされる．

またここで γ を α であらわすと，$\gamma = \dfrac{p_1\alpha + p_2}{q_1\alpha + q_2}$ となるから，

$$A(p_1x + p_2y)^2 + B(p_1x + p_2y)(q_1x + q_2y) + C(q_1x + q_2y)^2$$
$$= a^2(x - \alpha y)(x - \alpha^\sigma y) = a(ax^2 + bxy + cy^2)$$

がなりたつ．左辺の判別式は $(p_1q_2 - p_2q_1)^2(B^2 - 4AC) = a^2(B^2 - 4AC)$．これより $b^2 - 4ac = B^2 - 4AC$ となる．

以上の考察は

$$X = p_1x_1x_2 + p_2x_1y_2 + p_2'y_1x_2 + p_3y_1y_2 = (x_1, y_1)\begin{pmatrix} p_1 & p_2 \\ p_2' & p_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},$$

$$Y = q_1x_1x_2 + q_2x_1y_2 + q_2'y_1x_2 + q_3y_1y_2 = (x_1, y_1)\begin{pmatrix} q_1 & q_2 \\ q_2' & q_3 \end{pmatrix}\begin{pmatrix} x_2 \\ y_2 \end{pmatrix}$$

として出発すれば，一般の composition の場合にそのまま拡張できる．命題中の式はベクトルの外積のようになっているが，特に幾何学的な意味はないようである．

Section 2. Principal genus theorem と ternary form.

前 Sec. で述べた composition を通じて，与えられた判別式 D をもつ primitive な２次形式の SL(2, Z) 同値類が２次体 $F = \mathbf{Q}(D^{1/2})$ の狭義の ideal 類と同型な群をなす．また，ideal のノルムが到るところ局所ノルムであるという条件で規定される principal genus が，平方類になるという形で principal genus theorem が言い表される．もっとも，狭義類というような符号条件のついたものを出すには，composition の方にもそれに対応した性質を持たせなければならない．そのためには，composition の定義に用いられた行列 P, Q について

$$\begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix} > 0 \quad \text{および} \quad \begin{vmatrix} p_1 & p_2' \\ q_1 & q_2' \end{vmatrix} > 0$$

のなりたつことを要請すればよいのである．

以下 principal genus theorem を ternary form によって証明する Gauss の方法を解説するのであるが，Gauss は２次形式を $ax^2 + 2bxy + cy^2$ の形のものに限って考察し，$b^2 - ac$ を判別式といった．これは $D \equiv 1 \pmod 4$ でなければ $\frac{1}{4}D$ を判別式といっているだけで，やっていることの内容は本稿と変わらないが，$D \equiv 1 \pmod 4$ だと，判別式が変わらないかわり内容自体が少し食い違ってくる．その食い違いは大したことではないが，ここでは簡単のため $D \equiv 1 \pmod 4$ でないとして話を進める．

Principal genus theorem の ternary form を用いた Gauss の証明を，これから本 Sec. の終わりまで を述べる．（[3], art. 286）

Principal genus に属する２次形式 $F(T, U) = AT^2 + 2BTU + CU^2$, $(A > 0,\ B^2 - AC$ は $\frac{1}{4}D)$, について，もし，

$$A = \alpha^2 - 2\alpha'\alpha'', \quad 2B = -2(\alpha\beta - \alpha'\beta'' - \alpha''\beta'), \quad C = \beta^2 - 2\beta'\beta''$$

となる $\alpha, \alpha', \alpha''; \beta, \beta', \beta''$ が見つかれば，Sec. 1 の duplication の公式で，まず

$$P = \begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix} = \begin{pmatrix} 2\beta' & \beta \\ \beta & \beta'' \end{pmatrix}, \qquad Q = \begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix} = \begin{pmatrix} 2\alpha' & \alpha \\ \alpha & \alpha'' \end{pmatrix}$$

とすることにより，

$$-\begin{vmatrix} q_1 & q_2 \\ q_2 & q_3 \end{vmatrix} = -\begin{vmatrix} 2\alpha' & \alpha \\ \alpha & \alpha'' \end{vmatrix} = A,$$

$$\begin{vmatrix} p_1 & q_2 \\ p_2 & q_3 \end{vmatrix} + \begin{vmatrix} q_1 & p_2 \\ q_2 & p_3 \end{vmatrix} = \begin{vmatrix} 2\beta' & \alpha \\ \beta & \alpha'' \end{vmatrix} + \begin{vmatrix} 2\alpha' & \beta \\ \alpha & \beta'' \end{vmatrix} = 2B,$$

$$-\begin{vmatrix} p_1 & p_2 \\ p_2 & p_3 \end{vmatrix} = -\begin{vmatrix} 2\beta' & \beta \\ \beta & \beta'' \end{vmatrix} = C$$

および

$$\begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix} = \begin{vmatrix} 2\beta' & \beta \\ 2\alpha' & \alpha \end{vmatrix} = 2a, \quad \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix} = \begin{vmatrix} 2\beta' & \beta'' \\ 2\alpha' & \alpha'' \end{vmatrix} = -2b,$$

$$\begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix} = \begin{vmatrix} \beta & \beta'' \\ \alpha & \alpha'' \end{vmatrix} = c$$

がなりたつ。ここで

$$a = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}, \quad b = \begin{vmatrix} \alpha' & \beta' \\ \alpha'' & \beta'' \end{vmatrix}, \quad c = -\begin{vmatrix} \alpha & \beta \\ \alpha'' & \beta'' \end{vmatrix}$$

である。従って F は $2ax^2 - 2bxy + cy^2$ の duplication になる．また

$$P = \begin{pmatrix} p_1 & p_2 \\ p_2 & p_3 \end{pmatrix} = \begin{pmatrix} \beta' & \beta \\ \beta & 2\beta'' \end{pmatrix}, \quad Q = \begin{pmatrix} q_1 & q_2 \\ q_2 & q_3 \end{pmatrix} = \begin{pmatrix} \alpha' & \alpha \\ \alpha & 2\alpha'' \end{pmatrix}$$

としてみれば，

$$-\begin{vmatrix} q_1 & q_2 \\ q_2 & q_3 \end{vmatrix} = -\begin{vmatrix} \alpha' & \alpha \\ \alpha & 2\alpha'' \end{vmatrix} = A,$$

$$\begin{vmatrix} p_1 & q_2 \\ p_2 & q_3 \end{vmatrix} + \begin{vmatrix} q_1 & p_2 \\ q_2 & p_3 \end{vmatrix} = \begin{vmatrix} \beta' & \alpha \\ \beta & 2\alpha'' \end{vmatrix} + \begin{vmatrix} \alpha' & \beta \\ \alpha & 2\beta'' \end{vmatrix} = 2B,$$

$$-\begin{vmatrix} p_1 & p_2 \\ p_2 & p_3 \end{vmatrix} = -\begin{vmatrix} \beta' & \beta \\ \beta & 2\beta'' \end{vmatrix} = C$$

および

$$\begin{vmatrix} p_1 & p_2 \\ q_1 & q_2 \end{vmatrix} = \begin{vmatrix} \beta' & \beta \\ \alpha' & \alpha \end{vmatrix} = a, \quad \begin{vmatrix} p_1 & p_3 \\ q_1 & q_3 \end{vmatrix} = \begin{vmatrix} \beta' & 2\beta'' \\ \alpha' & 2\alpha'' \end{vmatrix} = -2b,$$

$$\begin{vmatrix} p_2 & p_3 \\ q_2 & q_3 \end{vmatrix} = \begin{vmatrix} \beta & 2\beta'' \\ \alpha & 2\alpha'' \end{vmatrix} = 2c$$

がなりたつから，F は $ax^2 - 2bxy + 2cy^2$ の duplication でもある．どちらの場合にも判別式の一致 $b^2 - 2ac = B^2 - AC$ のなりたつことは，やはり duplication の公式からわかる．

これで，残るのは，求める α, β, etc. の見出し方を示すことと，得られる form の少なくとも一方が primitive であることをいうために，a, c の少なくとも一方が奇であることを示すこととになった．

そのため，

$$-\begin{vmatrix} A & -B & C' \\ -B & C & B' \\ C' & B' & A' \end{vmatrix} = AB'^2 + 2BB'C' + CC'^2 + A'(B^2 - AC)$$

という式を見ると，この式の右辺は A', B', C' を適当に選んで 1 にできることがわかる．なぜなら，F が principal genus に属することから，

$$AB'^2 + 2BB'C' + CC'^2 \equiv 1 \pmod{D}$$

となる B', C' は選べるからである．このことはほとんど principal genus の定義といってもよいことである．すなわち，F のあらわす数は ideal のノルムと数のノルムとの積であり，今の場合 ideal のノルムの方が数のノルムと mod D で合同なのであるから，数のノルムの方を調節して全体を $\equiv 1 \pmod{D}$ にできるのである．このようにして，$F' = AT^2 - 2BTU + CU^2$ に項をつけ加えた ternary form

$$AT^2 + CU^2 + A'V^2 + 2B'UV + 2C'VT - 2BTU$$

が得られ，係数の行列式は -1 である．（Gauss は ternary form の行列式にマイナスをつけて定義しているので，この場合 行列式は 1 といっている．）Gauss の ternary form の標準形の議論より，行列式 -1 の indefinite ternary form は，$x^2 - 2yz$ に整同値である．すなわち

$$\begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix} \in SL(3, Z)$$

が存在して

$$AT^2 + CU^2 + A'V^2 + 2B'UV + 2C'VT - 2BTU$$
$$= (\alpha T + \beta U + \gamma V)^2 - 2(\alpha' T + \beta' U + \gamma' V)(\alpha'' T + \beta'' U + \gamma'' V)$$

がなりたつ．$V = 0$ とすれば

$$AT^2 - 2BTU + CU^2 = (\alpha T + \beta U)^2 - 2(\alpha' T + \beta' U)(\alpha'' T + \beta'' U).$$

これを展開すれば，この α, β, etc. がちょうど求めるものになっていることがわかる．すなわち，2次の行列の3次の行列による表現

$$\begin{pmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \\ \alpha'' & \beta'' \end{pmatrix} = \begin{pmatrix} A & -B \\ -B & C \end{pmatrix}$$

である．さらに，a, b, c は SL の 行列の小行列式になっているからそれらの公約数は 1 しかない．一方

$$\alpha'' a + \alpha b + \alpha' c = 0, \qquad \beta'' a + \beta b + \beta' c = 0,$$

がなりたつ．故に，もし a, c が共に偶ならば b は奇で，さらに α, β が共に偶となる．これは A, C が共に偶であることを意味し，不合理である．これで必要なことがすべて証明された．

Section. 3. Principal genus theorem の幾何学的証明.

有理数 a が判別式 D の2次体の数のノルムであるということは，$a = x^2 + Dy^2$ が有理解をもつということである．それは，x, y を分数表示して考えれば，$ax_1^2 = x_2^2 + Dx_3^2$ が Z で解を持つことと同じである．従って，principal genus theorem を証明するには，$ax_1^2 = x_2^2 + Dx_3^2$ がすべての素数 p について p 進整数環 Z_p の中で解を持てば Z で解を持つということをいえばよい．そこで，この Sec. では，もうすこし一般に，$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$, $(a_1a_2a_3 \neq 0)$, がすべての Z_p で自明でない（$x_1 = x_2 = x_3 =$

0 以外の）解を持てば，Z で自明でない解を持つということを，Sec. 2 とは全く別の幾何学的方法によって証明する．この方法は [2] で，Legendre によってはじめて発表されたものとして紹介されている．しかし，[2] の説明はあまりわかりやすいとはいえないので，少し形を変えて述べる．

準備として a_1, a_2, a_3 にいくつか条件をつけてもよいことをいう．まず a_1, a_2, a_3 は 1 以外に公約数を持たないとしてよい．次に，もし a_1 が平方因子を持ち，$a_1 = a_1'b^2$ となっていたとすれば，$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ の解 x_1, x_2, x_3 に対し bx_1, x_2, x_3 は $a_1'x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ の解である．逆に，後者の解 x_1, x_2, x_3 に対し，x_1, bx_2, bx_3 は前者の解である．さらに，もし a_1, a_2 が公約数を持ち，$a_1 = ba_1'$, $a_2 = ba_2'$ となっていたとすれば，$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ の解 x_1, x_2, x_3 に対し bx_1, bx_2, x_3 は $a_1'x_1^2 + a_2'x_2^2 + ba_3x_3^2 = 0$ の解である．逆に，後者の解 x_1, x_2, x_3 に対し，x_1, x_2, bx_3 は前者の解である．これらのことは，$\mathbf{Z}_p$ においてももちろんなりたつ．従って，a_1, a_2, a_3 はどれも平方因子を持たず，また，1 つの素数 p については，高々 1 つだけが p で割り切れるとしてよい．一方，すべての p について $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ が Z で解を持つという条件で証明するかわりに，ある有限個の p についてという条件のもとに証明できればそれで十分なことはもちろんである．

以上の要件をすべて取り入れた上で，目標の定理をあらためて書けば次のとおりである．

定理（Ternary diagonal form の Hasse 原理） どの 1 つも 0 でなく，平方因子をもたない有理整数 a_1, a_2, a_3 があり，1 つの素数 p についてはそのうちの高々 1 つしか割り切れないとする．このとき，もし不定方程式

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$$

が $2a_1a_2a_3$ を割り切るすべての素数 p について Z_p で解を持ち，さらに p_∞ についても（すなわち R でも）解を持てば，Z で解を持つ．

証明は Minkowski の格子点定理によるのであるが，局所的な解の存在を格子の性質であらわすためには，次の命題が有用である．

命題（加群上での2次形式の付値の最大値） $f(x_1, x_2, x_3) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ が Z_p 係数の2次形式で，a_1, a_2, a_3 のうち，p が奇素数ならばちょうど1つ，$p = 2$ ならば高々1つが p で割り切れ，しかも，どちらの場合も p^2 では割り切れないとし，$f(x_1, x_2, x_3) = 0$ は Z_p^3 で自明でない解を持つとする．このとき，p が奇ならば，Z_p^3 の部分加群 L_p であって，$(Z_p^3 : L_p) = p$，かつ f の $(x_1, x_2, x_3) \in L_p$ での p 進付値の最大値が高々 p^{-1} であるものが存在する．また $p = 2$ ならば，Z_2^3 の部分加群 L_2 であって，$(Z_2^3 : L_2) = 4$，かつ f の $(x_1, x_2, x_3) \in L_2$ での2進付値の最大値が高々 4^{-1} であるものが存在する．

まず $p \neq 2$ とする．$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ の1組の自明でない解を b_1, b_2, b_3 とし，b_1, b_2, b_3 のすべては p で割り切れず，また a_1, a_2, a_3 のうち p で割り切れるのは a_3 であるとすれば，$a_1b_1^2 + a_2b_2^2 + a_3b_3^2 = 0$ により，もし b_3 が p で割り切れなければ，$a_3b_3^2$ の p 進付値は p^{-1} であるから b_1 も b_2 も p で割り切れない．また，b_3 が p で割り切れれば，b_1, b_2 が共に p で割り切れることはないという仮定より，b_1, b_2 は共に p で割り切れない．すなわち，b_1, b_2 は常にどちらも p で割り切れない．そこで $b = (b_1, b_2, b_3)$，$b' = (0, 0, 1)$ $(\in Z_p^3)$ とおき，さらに $L_p = bZ_p + b'Z_p + pZ_p^3$ とすれば，この L_p が求めるものである．次に $p = 2$ のときは，やはり $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$ の1組の

自明でない解を b_1, b_2, b_3 とし，b_1, b_2, b_3 のすべては 2 で割り切れないとしたとき，$b = (b_1, b_2, b_3)$, $L_2 = bZ_2 + 2Z_2^3$ が求めるものである．

命題の証明ができたから，定理の証明に入る．Z^3 $(\subset R^3)$ の元であって $2a_1a_2a_3$ を割り切るすべての p について命題にいう L_p に入るもののなす加群を L とする．これは R^3 の格子群である．命題より R^3/L の体積 v は $a_1a_2a_3$ が 2 で割り切れるか割り切れないかに従って $|2a_1a_2a_3|$ または $|4a_1a_2a_3|$ である．ここで

$$|a_1x_1^2 + a_2x_2^2 + a_3x_3^2| < v$$

という不等式で決まる R^3 内の領域 B を考える．定理の条件により，a_1, a_2, a_3 は全部同符号ではないから，$a_1 > 0$, $a_2 > 0$, $a_3 < 0$ としてひとまず考えると，B の中には

$$|a_1x_1^2 + a_2x_2^2| < v, \qquad |a_3x_3^2| < v$$

で定まる領域（楕円柱）が確かに含まれ，その体積は $a_1a_2a_3$ が 2 で割り切れるか割り切れないかに従って

$$\frac{\pi}{2^{3/2}}\cdot 8v \qquad \text{または} \qquad \frac{\pi}{2}\cdot 8v$$

であって，これは R^3/L の体積の 8 倍より大きい．故に Minkowski の定理より B は $|a_1b_1^2 + a_2b_2^2 + a_3b_3^2| < v$ を満足する $(0, 0, 0)$ 以外の $(b_1, b_2, b_3) \in L$ を含む．しかし，$a_1b_1^2 + a_2b_2^2 + a_3b_3^2$ は命題より v で割り切れるから，$a_1b_1^2 + a_2b_2^2 + a_3b_3^2 = 0$ でなければならない．a_1, a_2, a_3 は上の推論では対称的に扱われているから，上で行った符号の指定は一般性を損なわない．これで定理は証明された．

以上の証明は，局所解から大局解を構成する方法を大変透明に示すものであるが，一般の数体の場合に拡張することは意外に困難である．補助に用いた命題とか，a_1, a_2, a_3 の p による割り切れかたにつけた条件などは何でもなく処理できるのであるが，B のような凸形を十分大きな体積を持つよ

うにとることができなくなるのである．そのあたりの状況の解明を可能にするような，新しいアイデアが望まれる．

Legendre は Sec. で述べた定理によって，平方剰余の相互法則が証明できると主張した．しかし，Gauss はその方法が不完全であることを見出し，[3] の art. 296 ~ 297 において，かなり強い調子で批判している．

参　考　書

[1] P. Bachmann, Niedere Zahlentheorie, Teubner, 1910.

[2] J. W. S. Cassels, Rational quadratic forms, Academic Press, 1978.

[3] C. F. Gauss, Disquisitiones arithmeticae, Fleischer, 1901.

[4] 高木貞治，初等整数論講義，共立出版，1931.